

# Backup-Strategien gegen Datenverlust

- Gerät geht kaputt
- Gerät geht verloren
- Gerät wird geklaut/beschlagnahmt
- Wohnung brennt ab

# Wo kann man Backups speichern?

## Externe Festplatte

- am besten mit USB 3.0
- muss mindestens so groß sein wie die Festplatte in eurem PC

## Alte, ausgebaute Festplatte mit USB-to-SATA-Adapter

- ist billiger als eine neue externe Festplatte (Adapter kostet ~7€)

# Wo kann man Backups speichern?

## Cloud

- Vorteil:
  - Festplatten gehen vllt mit dem Gerät verloren; besonders wenn man sie in derselben Wohnung lagert
- Nachteile:
  - große Cloud-Accounts sind teurer als externe Festplatten
  - "Clouds are just somebody else's Computer" -> aber selbst-hosten oder cloud.0x90.space benutzen ist evtl ne Option

# Wo kann man Backups speichern?

## Tails-Sticks

- Einfacher Weg einen verschlüsselten USB-Stick zu erstellen
- Insbesondere, weil er sich selbst öffnen kann; dadurch ist man im Krisenfall schnell einsatzfähig
- Nicht viel Speicherplatz, aber genug für Passwort-Datenbanken + PGP-Schlüssel

# Was für Daten sollten ins Backup?

- Bilder, Dokumente, etc. -> idR einfach Dateien die rumliegen
- Kontakte auf Smartphones -> kann man als .vcf-Datei exportieren oder mit einer Cloud synchronisieren
- Zugangsdaten -> Passwort-Manager-Datenbanken, Textdateien in denen Passwörter stehen, Recovery-Codes für 2-Faktor-Authentifizierung

# Was für Daten sollten ins Backup?

- kostenpflichtige Anwendungen, Spiele, Apps -> Installations-Dateien: setup.exe, .apk bei Android, etc., evtl Lizenzschlüssel für Photoshop oder so
- Anwendungs-Daten -> z.B. Signal-Datenbank, Delta Chat-Datenbank, Browser-Bookmarks.

-> Was würdet ihr persönlich backuppen wollen?

## **Simpleste Lösung: einfach einzelne Dateien auf eine externe Festplatte kopieren**

Vorteil: braucht kein Spezialwissen

Nachteile:

- Manueller, regelmäßiger Aufwand
- Anwendungs-Daten sind zB auf Android nicht als Dateien zugänglich, und auf Windows nicht immer leicht zu finden; man kommt also damit nicht an alle Daten ran die man braucht

## **Sauberste Lösung: anderes Betriebssystem booten und ganze Festplatte kopieren**

Laptops & PCs

- Live-Stick booten (z.B. Tails)
- die gesamte Festplatte auf eine größere, externe Festplatte kopieren
- zB mit dem Kommandozeilen-Tool dd



## **Sauberste Lösung: anderes Betriebssystem booten und ganze Festplatte kopieren**

Android

- Recovery-tool TWRP kann die verschiedenen Partitionen auf die micro-SD-Karte schreiben.
  - Solche Backups lassen sich aber nur auf demselben Gerät restoren
  - und auf anderen Geräten mit demselben Modell nur durch einen Trick

## **Sauberste Lösung: anderes Betriebssystem booten und ganze Festplatte kopieren**

Nachteile:

- manueller, regelmäßiger Aufwand
- TWRP draufspielen und Live-Sticks booten muss man erstmal können

## **Spezielle Backup-Programme wie Kopia, Smart Switch, oder Borgbackup**

Vorteile:

- Je nach tool Benutzungsoberfläche für Leute ohne Spezialwissen
- Sparen idR Kopierzeit und Speicherplatz durch Kompression & Deduplikation
- Oft eingebaute Verschlüsselung

## **Spezielle Backup-Programme wie Kopia, Smart Switch, oder Borgbackup**

Nachteile:

- undurchsichtig was genau passiert
- eigentlich muss man trotzdem drauf achten, dass auch die Anwendungs-Daten mit gebakuppt werden
- idR trotzdem manueller, regelmäßiger Aufwand
- Man braucht das Tool zum wiederherstellen der Daten

## **Cloud-Lösung: automatisch synchronisieren**

Am besten ownCloud/nextcloud, nicht Google Drive oder Dropbox

Vorteile:

- Backups sind immer aktuell
- man muss nicht regelmäßig dran denken
- alle anderen File Sharing & Features

## **Cloud-Lösung: automatisch synchronisieren**

Nachteile:

- Storage ist teuer
- Keine Anwendungs-Daten (außer über komplexe Verknüpfungen)
- Man muss dem Cloud-Provider vertrauen

Verschlüsselter Container hilft, aber dann geht Sharing nicht

## Hybrid-Lösung: Cloud-Lösung + Tails-Stick mit Zugangsdaten

- Passwort-Manager, PGP-Keys, SSH-Keys, und anderes Identitäts-Material auf einem Tails-Stick speichern (im persistenten Speicher).
- Am besten mehrere Tails-Sticks, die man bei Freunden versteckt
- Anwendungs-Daten:
  - kann man entweder in real-time in die Cloud schieben
  - oder regelmäßig mal auf einen Tails-Stick schieben.

## **Hybrid-Lösung: Cloud-Lösung + Tails-Stick mit Zugangsdaten**

### Vorteile:

- Daten die auf den Tails-Stick sollen ändern sich selten; Backups sind also fast immer aktuell
- man muss es nur einmal einrichten und dann nicht regelmäßig dran denken

### Nachteile

- Alle Nachteile von Clouds



## Tipps um regelmäßig dran zu denken

- Regelmäßiger Kalender-Reminder
- Über Nacht laufen lassen. wenn nicht - was macht man parallel?
- Klebezettel am Spiegel, damit man abends beim Zähneputzen dran denkt

# Datenexport bei Anwendungen

Je nach Programm eigene Export- oder Synchronisierungs-Funktion. Beispiele:

- Telegram hat einfach alles auf dem Server, und wenn man sich mit der Sim-Karte einloggt kommt man an die Daten
- Bei Signal auf Android muss man regelmäßige Backup-Exports anschalten, um die Message History zu save;
  - man braucht genug Speicherplatz auf dem Handy, SD-Karte geht nicht

# Datenexport bei Anwendungen

Je nach Programm eigene Export- oder Synchronisierungs-Funktion. Beispiele:

- Bei Delta Chat kann man das Backup auf allen Geräten exportieren
  - E-Mail-Passwort & Verschlüsselungs-Keys sind da mit drin
  - lieber Backup importieren als mit dem Passwort wieder einloggen, damit sich die Verschlüsselungs-Keys nicht ändern
- Firefox bietet Mozilla Sync an, um Lesezeichen, Chronik, gespeicherte Passwörter etc. über einen Mozilla-Account zu synchronisieren

# Datenexport bei Anwendungen

- Bei Laptops/PCs liegen die Anwendungs-Daten auch irgendwo auf der Festplatte
  - z.B. bei Windows unter %APPDATA%, bei Linux oft unter ~/.config/, etc.
- Bei Anwendungs-Daten, Datenbanken, etc.
  - Darauf achten dass kein Programm mehr läuft, das die Dateien bearbeitet, während man sie kopiert -> Inkonsistenzen
  - Dann funktioniert das Backup evtl nicht wenn man es braucht.
  - Die export-Funktion der Anwendung selbst achtet da allerdings darauf.

# Kleingruppen

*3-5 Leute pro Gruppe, 30 Minuten*